Abstract

A device key 46 is implemented on a drive 4 side. To securely transmit the device key 46 to a host 5, the device key 46 is encrypted with a bus key. The host 5 side decrypts the device key with the bus key. A medium unique key calculating block 55 calculates a medium unique key with an MKB 12, a medium ID, and the decrypted device key 46. When the calculated medium key is a predetermined value, the drive 4 is revoked and the process is stopped. The medium unique key is supplied to an encrypting/decrypting module 54. A content key is obtained with an encrypted title key 14 and a CCI 15. With the content key, an encrypted content is decrypted and a content that is recorded is encrypted.